(12) **UK Patent Application** (19) **GB** (11) **2 354 137** (13) **A**

(43) Date of A Publication 14.03.2001

(21) Application No 9910845.8

(22) Date of Filing 10.05.1999

(71) Applicant(s)
3Com Corporation
(Incorporated in USA - Delaware)
5400 Bayfront Plaza, M/S 1308, Santa Clara,
California 95052-8145, United States of America

(72) Inventor(s)
Simon Peter Valentine
Lee Walker
Christopher Robert Linzell

(74) Agent and/or Address for Service
Brookes & Martin
High Holborn House, 52-54 High Holborn, LONDON,
WC1V 6SE, United Kingdom

(51) INT CL⁷
H04L 12/24 12/26 // H04L 12/56

(52) UK CL (Edition S)
H4P PPG

(56) Documents Cited
WO 97/31458 A1   WO 89/07377 A1   JP 040152733 A
US 5732086 A   US 5586267 A   US 5421024 A
US 4545013 A

(58) Field of Search
UK CL (Edition Q) H4P PPG
INT CL⁶ H04L 12/24 12/26 12/56
Online: WPI, EPODOC, JAPIO

(54) Abstract Title
Network supervisory system where components are instructed to poll their neighbours to obtain address information

(57)   A network is made up of a number of components 12,13,14 connected by links 16 between ports of the components, wherein each component or port has an address. At least some of the components or their have means, such as agents, for storing the address of the remote port or component to which they are connected. This information can be obtained from messages transmitted into the port from the remote component.

Where a component eg.13B does not have the addresses of the remote components eg.12C-E,14 or ports to which its ports are connected for all of its ports it "pings" the remote component eg.14 (ie sends it a message requesting that it respond with its address information) from the ports lacking remote address information. In this way it is ensured that all components which can learn their neighbouring components addresses do so. From this data a network map may be constructed.

A supervisory system 11 may control the address gathering and construct the network map.
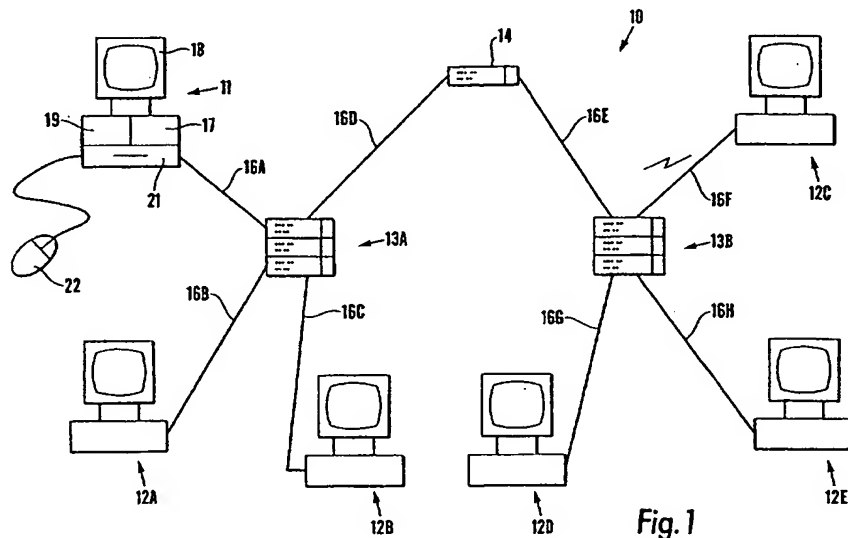
Fig. 1

GB 2 354 137 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

Fig.1

Fig.2

INTERROGATE AGENTS OF EACH COMPONENT TO ESTABLISH WHICH PORTS HAVE RECEIVED ADDRESS OF REMOTE COMPONENTS OR PORTS TO WHICH THEY ARE CONNECTED — 100

FOR EACH COMPONENT, ESTABLISH WHICH PORTS HAVE INCOMPLETE ADDRESS INFORMATION — 101

FOR EACH COMPONENT, FOR EACH OF THE PORTS WITH INCOMPLETE ADDRESS INFORMATION, REMOTELY POLL THE REMOTE COMPONENT TO WHICH IT IS CONNECTED — 102

INTERROGATE AGAIN AGENTS OF EACH COMPONENT TO ESTABLISH ADDRESS OF REMOTE COMPONENTS OR PORTS TO WHICH EACH PORT IS CONNECTED — 103

STORE INFORMATION RELATING TO COMPONENTS, PORTS AND REMOTE PORTS — 104

ACCESS INFORMATION — 105
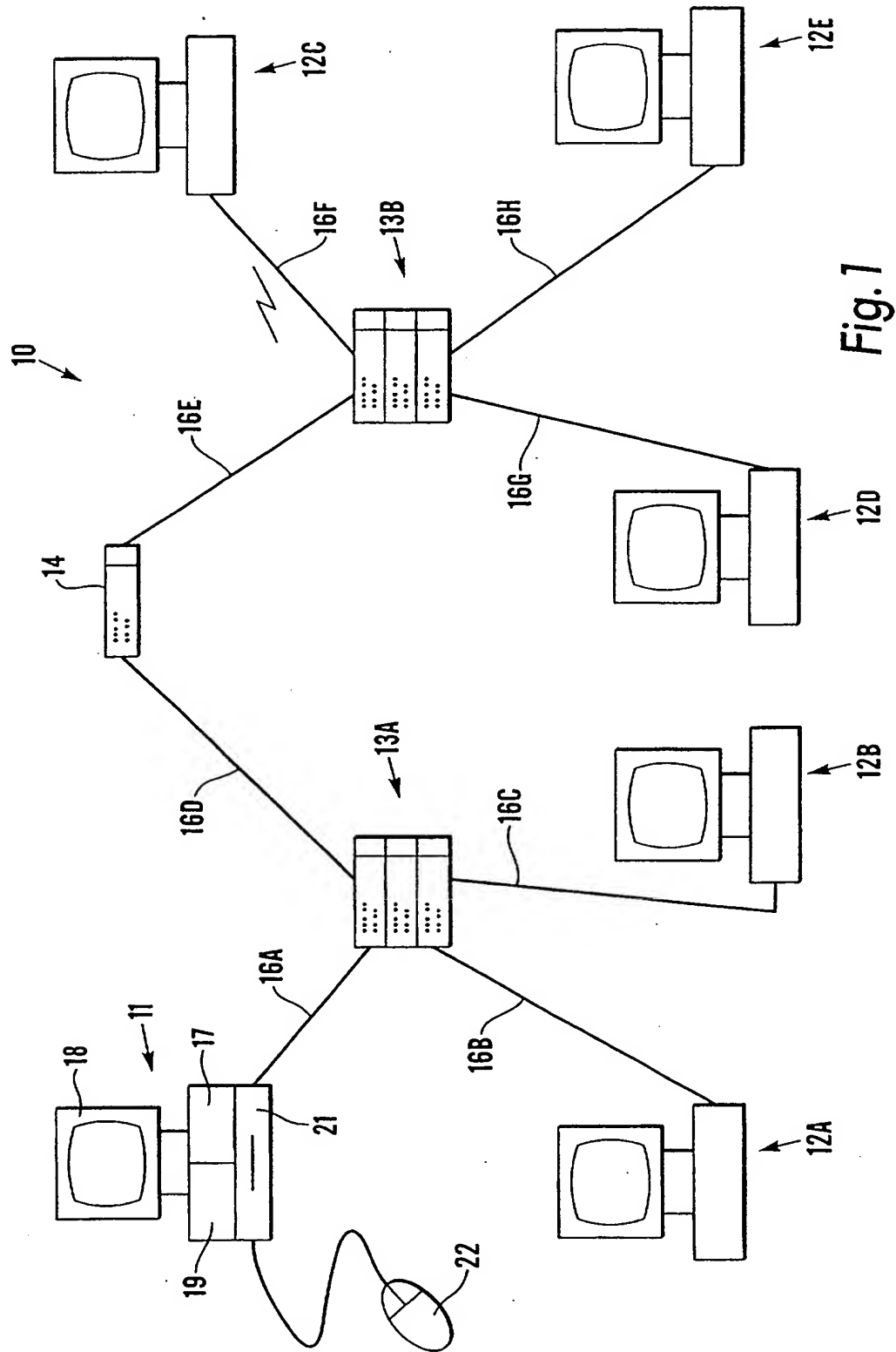
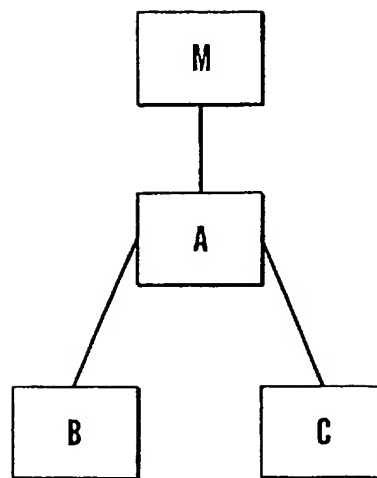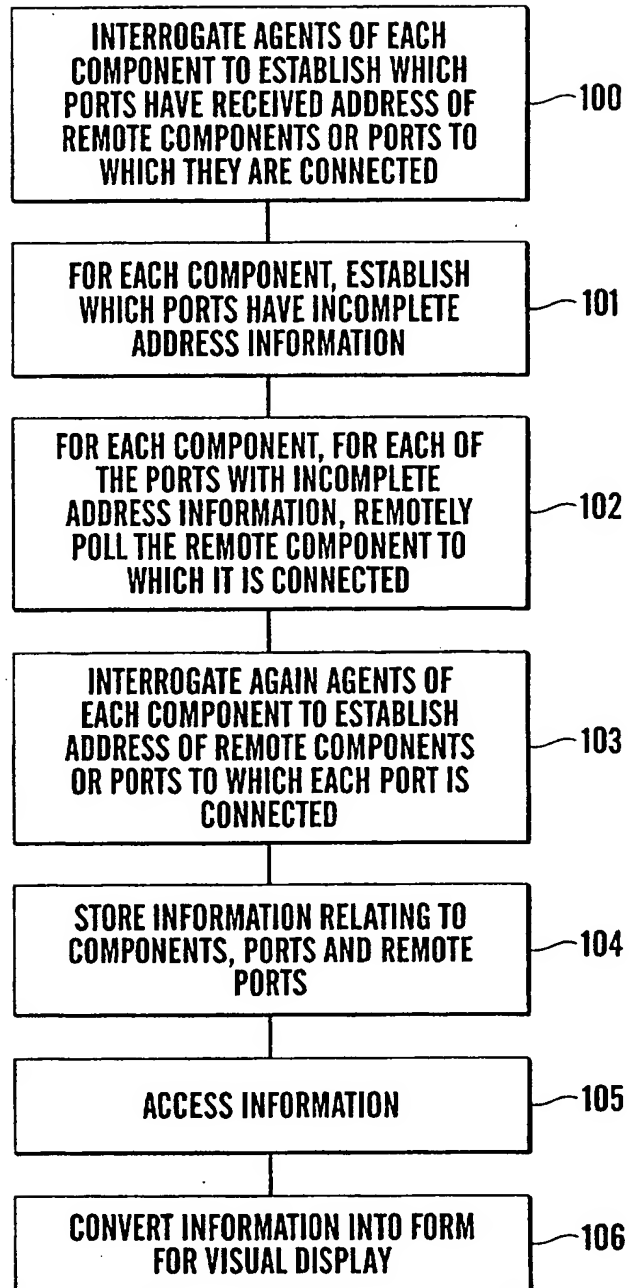CONVERT INFORMATION INTO FORM FOR VISUAL DISPLAY — 106

Fig.3

SUPERVISING A NETWORK

BACKGROUND OF THE INVENTION

5

The present invention relates to supervising a network, that is a network of electronic
components comprising, for example, workstations, personal computers, servers, hubs,
routers, bridges, switches, (hereinafter referred to as components of the network), and
links between these components which may be in the form of physical cable or wireless

10 links. The network may be a local area network (LAN), wide area network (WAN) or
other types and may operate in accordance with any desired protocol.

After such a network has been installed, it is desirable for the person appointed
network manager to be able to understand the technical operation of the network.

15 In known network management systems, the manner in which the relevant data is
retrieved from the managed devices, compiled and displayed has been problematic in
several respects. Firstly, the data received from each of the managed devices is simply
compiled and displayed as a list of data for the user to interpret. Secondly, the data
does not provide information about unmanaged devices. Thirdly, information about a

20 given network device, such as the type of device, location of the device on the network
and operating speed of the device, may be contained in different sections of the
compiled data. Consequently, conventional systems are cumbersome and difficult to
use.

GB9910843.3, GB9901961.3, GB9910844.1, GB9910962.1,

25 In our co-pending UK patent applications numbers GB9910838.3, GB9910837.5, GB9910839.1,
GB9910840.9, (our case numbers 2345, 2348, 2349, 2351, 2450, 2451, 2455, 2456 filed
concurrently herewith) and which are incorporated herein, we describe various
arrangements for providing automatic interrogation of the network to thereby produce
a network map which may be displayed on a visual display unit showing the

1

components and links between the components. At its simplest, and where the component is a "managed" component, this is usually provided by interrogation using a known protocol, such as the SNMP protocol, of the so-called 'agent' of each component which stores the components unique MAC address, the type of component

5 and the MAC addresses the components which are connected to the ports directly or indirectly.

However, the agent of each component can only store the MAC address of the remote component (or the port address) to which a particular port is connected after it has

10 received a signal originating from that remote component which includes the relevant address. Data signals usually carry both source and destination addresses but until the source address is received, it cannot be stored by the agent. In particular operations of the network, source address headed data may generally only pass in one direction. Thus there will be a number of ports which will not have received a signal sourced

15 from the remote component to which they are attached and which therefore will not know the MAC address of that remote component. As a result, it is impossible to provide a network map or deduce properly the topology of the network as it is necessary to know which ports of which component are attached to each other.

20 The present invention seeks to address this problem.

It should also be noted that some components (usually switches and hubs) use the component address as a source address whereas other components (such as routers) use the port address as the sourced address.

25

SUMMARY OF THE INVENTION

The present invention provides A method of supervising a network, which network comprises a plurality of components having ports, at least some of which ports are

2

connected by links to ports on other components, at least one component including an agent to ascertain the source addresses of the remote component or port to which each of its ports is connected when data is received from the relevant remote component, said method comprising:

5   interrogating said at least one component to establish which ports of the component have received the source address of the relevant remote component or its port to which they are connected by a link directly or indirectly;
and in respect of at least one of the other ports of said component, remotely polling the remote component to which it is connected via said port to cause said remote
10   component to return a data signal including the address to that port, whereby the source address of the relevant remote component or its port can be identified.

The present invention also provides network supervising apparatus for supervising a network comprising a plurality of components having ports, at least some of which
15   ports are connected by links to ports on other components, at least one component including an agent to ascertain the source addresses of the port of the remote component or port to which each of its ports is connected when data is received from the relevant remote component, said apparatus comprising:
        a processor unit to interrogate said at least one component to establish which
20   ports of the component have received the source address of the relevant remote component or its port to which they are connected by a link;
and in respect of at least one of the other ports of said component, to remotely poll the remote component to which it is connected via said port to cause said remote component to return a data signal including the address to that port, whereby the
25   source address of the relevant remote component or its port can be identified.

The present invention also provides a computer program on a computer readable medium for us in supervising a network comprises a plurality of components having ports, at least some of which ports are connected by links to ports on other

3

components, at least one component including as agent to ascertain the source addresses of the port of the remote component or port to which each of its ports is connected when data is received from the relevant remote component, said program comprising:

5   program means for interrogating said at least one component to establish which ports of the component have received the source address of the relevant remote component or its port to which they are connected by a link;

          program means for causing, in respect of at least one of the other ports of said component, remote polling of the remote component which is connected via said port 10   to cause said remote component to return a data signal including the address to that port;

          and program means to thereby identify the source address of the relevant remote component or its port.

15   BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the invention will now be described by way of example only with reference to the accompanying drawings in which:-

20   Figure 1 is a diagrammatic view of a network incorporating a preferred embodiment of the invention,
Figure 2 is a detail of part of the network, and
Figure 3 sets out details of the program steps.

25   DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring to Figure 1 there is shown a network 10 comprising a plurality of components in the form of a network supervisor's workstation or computer 11, other workstations 12B - E, hubs 13A, 13B, and switch 14. The network is a simple

4

network and is set out for purposes of illustration only. Other configurations and arrangements, may be used.

5
The components are connected together by means of links 16A - H which may be hard wired and utilise any desired protocol, and link 16F which is a wireless link.

10
The network supervisor's workstation includes, in addition to a visual display unit 18, a central processing unit or signal processor 19, a selector which may be in the form of a mouse 22, a program store 21 which may comprise, for example, a CD drive, a floppy disk drive or a zip drive, and a memory 17 for storing a program which may have been loaded from the program store 21 or downloaded for example via Internet from a website.

15

20
By means which is disclosed in the co-pending patent applications referred to above, the network supervisor's computer 11 may interrogate and analyse the network, and store in the memory 17 the information relating to the components within the network and the links between the components. In essence, most quality components include a so-called agent which stores information about the component such as its unique MAC number, its ID which identifies what the component is and what model type it is, how many ports it has and how they are connected directly or indirectly, and the address to which at least some of the ports are connected. The computer 11 interrogates the agents of each component.

25
In order to clearly understand the invention it is necessary to understand a little more about the agent in managed components and the ports in those components. In managed components, each component or port will have a unique address. When that port directly communicates with another component (ie provides information originating with that port or its component - not simply forwarding or switching a signal received from elsewhere) it will forward its address to that component, (ie the

5

source address - it forms part of the header of the data signal). Thus in the part of the network illustrated in Figure 2, component M is connected by a link to component A, and component A is connected by links to components B and C, (for the purpose of this explanation we are ignoring other parts of the network). A, B and C are switches and M is a management station (eg the network supervisor's computer 11). Typically, M will be the only component to directly communicate with A, B and C, (interrogating them for management information). Consequently, packets that have as a source address A, B or C will always be going in the direction of M. This means that A will learn the addresses of B and C, but B and C will not learn the address of A.

In order to determine the topology of the network it is necessary to interrogate each managed component to establish for each port, the MAC address of the remote component or port to which it is connected. However, as set out above, components B and C will <u>not</u> know the address of A because data originating from A has not passed in that direction.

It is thus impossible to accurately construct a network tree with any degree of certainly in this situation because some of the information is missing. This situation arises in a switched environment where data commonly passes in one direction only rather than a shared environment in which packets of data are forwarded on all ports.

The present invention provides an arrangement to deal with this problem. During the initial interrogation phase when the computer M is interrogating all of the components of the network so as to determine their interconnections and to produce a network tree, it will interrogate the agent of each component which in the case of B and C will have incomplete information, that is, it will not know the address of A. In order to force B and C to learn the MAC addresses of A, we use remote poll (PING). By remote polling, one effectively drives the remote component to send a signal back to oneself. This can be done selectively in order to obtain just enough information to

6

build the tree. In the example shown in Figure 2, it will be sufficient to direct B to PING A and for C to PING A.

In essence, M will access the agent of component A, to determine that A is connected to B and C. It will then interrogate the agent of B, determine that the component to which it is connected is undetermined, the program will cause B to PING A thereby causing it to return a signal to B at which point the agent of B will be able to determine the address A to which B is connected. A similar procedure is carried out with regard to component C.

There are cases where the relevant port of a managed component does not in fact remember addresses or that address function has been switched off. Therefore the port will never learn the MAC addresses of any of the other managed components.

In such a case, if the component meets the following three criteria:

1. address learning is disabled on one port only,
2. remote poll is successful between that component and a second component,
3. the component still does not learn the MAC address of the second component.

then it can be assumed that it must be the non-learning port that is linked directly or indirectly to the second component. This can be used in establishing the topology of the network.

We have described how the network may be supervised. The method of the invention may be carried out under the control of the network supervisor's workstation or computer and in particular by means of a program controlling the signal processor

7

apparatus of that computer or elsewhere in the system.

The program for controlling the operation of the invention may be provided on a computer readable medium, such as a CD, or a floppy disk, or a zip drive disk carrying the program or their equivalent, or may be provided on a computer or computer memory carrying the website of, for example, the supplier of the network products. The program may be downloaded from whichever appropriate source and used to control the processor to carry out the steps of the invention as described.

The program may include (see Figure 3),

program means (100) for interrogating said at least one component to establish which ports of the component have an address of a remote component to which they are attached by a link,

program means (101) for establishing, for each component, which ports have incomplete address information,

program means (102) for causing, in respect of these ports with incomplete address information, remote polling of the remote component via the relevant port to cause said remote component to return a data signal with source address to that port,

program means (103) for interrogating the component again to establish the addresses of the remote component or ports to which each port is connected,

program means (104) to cause the information to be stored,

program means (105) to access that information, and

program means (106) to convert the information into a form for visual display.

The invention is not restricted to the details of the foregoing example.

CLAIMS

1.   A method of supervising a network, which network comprises a plurality of components having ports, at least some of which ports are connected by links to ports on other components, at least one component including an agent to ascertain the source addresses of the remote component or port to which each of its ports is connected when data is received from the relevant remote component, said method comprising:

interrogating said at least one component to establish which ports of the component have received the source address of the relevant remote component or its port to which they are connected by a link;

and in respect of at least one of the other ports of said component, remotely polling the remote component to which it is connected via said port to cause said remote component to return a signal including the address to that port, whereby the source address of the relevant remote component or its port can be identified.

2.   A method as claimed in claim 1 in which remote polling is carried out in respect of all of said other ports of said component.

3.   A method as claimed in claim 1 or claim 2 including deducing the topology of the network including the links between each component by identifying the addresses of the components or ports to which each port of each component is connected.

4.   A method as claimed in any of claims 1 to 3 in which, after remote polling, the port does not store an address, determining that a non-learning port is connected to the remote component.

5.   Network supervising apparatus for supervising a network comprising a plurality of components having ports, at least some of which ports are connected by

9

links to ports on other components, at least one component including an agent to ascertain the source addresses of the port of the remote component or port to which each of its ports is connected when data is received from the relevant remote component, said apparatus comprising:

a processor unit to interrogate said at least one component to establish which ports of the component have received the source address of the relevant remote component or its port to which they are connected by a link;

and in respect of at least one of the other ports of said component, to remotely poll the remote component to which it is connected via said port to cause said remote component to return a signal including the address to that port, whereby the source address of the relevant remote component or its port can be identified.

6. Apparatus as claimed in claim 5 in which the processor unit carries out remote polling in respect of all of said other ports of said component.

7. Apparatus as claimed in claim 5 or claim 6 in which the processor unit deduces the topology of the network including the links between each component by identifying the addresses of the components or ports to which each port of each component is connected.

8. Apparatus as claimed in any of claims 5 to 7 in which, the processor unit, after remote polling, determines that the remote component is connected to a non-learning port if the port does not store an address.

9. A computer program on a computer readable medium, said computer program comprising software for performing the steps of any of claims 1 to 4.

10. A computer program on a computer readable medium for us in supervising a network comprises a plurality of components having ports, at least some of which

10

ports are connected by links to ports on other components, at least one component including as agent to ascertain the source addresses of the port of the remote component or port to which each of its ports is connected when data is received from the relevant remote component, said program comprising:

5   program means for interrogating said at least one component to establish which ports of the component have received the source address of the relevant remote component or its port to which they are connected by a link;

program means for causing, in respect of at least one of the other ports of said component, remote polling of the remote component which is connected via said port 10   to cause said remote component to return a signal including the address to that port;

and program means to thereby identify the source address of the relevant remote component or its port.

11.   A computer program as claimed in claim 10 in which remote polling is carried 15   out in respect of all of said other ports of said component.

12.   A computer program as claimed in claim 10 or claim 11 including program means to deduce the topology of the network including the links between each component by identifying the addresses of the components or ports to which each port 20   of each component is connected directly or indirectly.

13.   A computer program as claimed in any of claims 10 to 12 including program means to determine that the remote component to which that port is attached is connected to a non-learning port if, after remote polling, the port does not store an 25   address.

11

| Application No: | GB 9910845.8 | Examiner: | Owen Wheeler |
| Claims searched: | 1-13 | Date of search: | 11 November 1999 |

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

  UK Cl (Ed.Q): H4P (PPG)

    Int Cl (Ed.6): H04L: 12/24, 12/26, 12/56

Other: Online: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A	WO 97/31458 A1 [HAL]	
A	WO 89/07377 A1 [NETWORK EQUIPMENT TECHNOLOGIES]	
A	JP 040152733 A [RICOH] See abstract.	
A	US 5732086 A [LIANG]	
A	US 5586267 A [CHATWANI]	
A	US 5421024 A [FAULK]	
A	US 4545013 A [LYON]	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
		E	Patent document published on or after, but with priority date earlier than, the filing date of this application.
&	Member of the same patent family		

An Executive Agency of the Department of Trade and Industry